CLAIMS

What is claimed is:

1. An electronic device including an autonomous memory checker for runtime security assurance, the electronic device comprising:

a controller;

a memory reference file coupled to said controller; and

an authentication engine coupled to said controller wherein a check is performed during runtime operation of the electronic device comparing a real-time reference value corresponding to information stored in memory to a memory reference value.

2. The electronic device as recited in claim 1 wherein said check is performed periodically during runtime operation of the electronic device.

3. The electronic device as recited in claim 1 wherein said check is performed at random times during runtime operation of the electronic device.

4. The electronic device as recited in claim 1 further including a clock control block coupled to said authentication engine, said memory reference file, and said controller.

5. The electronic device as recited in claim 4 further including a direct memory access (DMA) controller coupled to said authentication engine and said controller.

6. The electronic device as recited in claim 5 further including a timing module coupled to said controller.

7. The electronic device as recited in claim 1 wherein said memory reference value is generated corresponding to trusted information stored in memory and wherein said memory reference value is stored in said memory reference file.

8. The electronic device as recited in claim 7 wherein said trusted information stored in memory is processed by said authentication engine to generate said memory reference value.

9. The electronic device as recited in claim 8 wherein said information stored in memory is processed by said authentication engine to generate said real-time reference value, and wherein said information stored in memory has not been modified if said memory reference value is identical to said real-time reference value.

10. A method of operating an electronic device for runtime security assurance comprising the steps of:

storing trusted information in memory;

providing said trusted information to an authentication engine;

generating a memory reference value corresponding to said trusted information;

storing said memory reference value in a memory reference file;

operating the electronic device in runtime mode;

providing memory content corresponding to memory locations where said trusted information was stored to said authentication engine during runtime operation of the electronic device;

generating a real-time reference value; and

comparing said real-time reference value to said memory reference value.

11. The method as recited in claim 10 wherein said step of generating a memory reference value corresponding to said trusted information further includes a step of generating said reference value with a hardware authentication engine.

12. The method as recited in claim 10 further including the steps of:

continuing runtime operation of the electronic device when said real-time reference value is identical to said memory reference value; and

signaling an error when said real-time reference is not identical to said memory reference value.

13. The method as recited in claim 12 further including a step of repeating a runtime check process comprising the steps of generating a real-time reference value from memory content corresponding to memory locations where said trusted information was stored and comparing said real-time reference value to said memory reference value.

14. The method as recited in claim 13 further including a step of running said runtime check process in a background of runtime operation of the electronic device.

15. The method as recited in claim 14 further including a step of randomizing when said runtime check process occurs during runtime operation of the electronic device.

16. A method of operating an electronic device for runtime security assurance comprising the steps of:

providing trusted information stored in memory to be hashed to an autonomous memory checker during a boot mode;

instructing said autonomous memory checker to hash said trusted information during said boot mode;

generating reference hash values from said trusted information;

storing said reference hash values to a memory reference file within said autonomous memory checker;

fetching said trusted information from memory during runtime for hashing by said autonomous memory checker;

generating runtime hash values with said trusted information retrieved during runtime;

comparing said reference hash values to said runtime hash values; and

signaling an error when said reference hash values differ from said runtime hash values to indicate that said trusted information has been modified.

17. The method as recited in claim 16 further including a step of repeating randomly the steps of:

fetching said trusted information from memory during runtime for hashing by said autonomous memory checker;

generating runtime hash values with said trusted information retrieved during runtime;

comparing said reference hash values to said runtime hash values; and

signaling an error when said reference hash values differ from said runtime hash values to indicate that said trusted information has been modified.

18. The method as recited in claim 16 wherein said step of providing trusted information stored in memory to be hashed to an autonomous memory checker during a boot mode includes a step of fetching said trusted information from a plurality of memory blocks.

19. The method as recited in claim 18 further including a step of continuing runtime operation of the electronic device when said runtime hash values are identical to said reference hash values.